PATENT ABSTRACTS OF JAPAN

(11)Publication number : 05-327693
(43)Date of publication of application : 10.12.1993

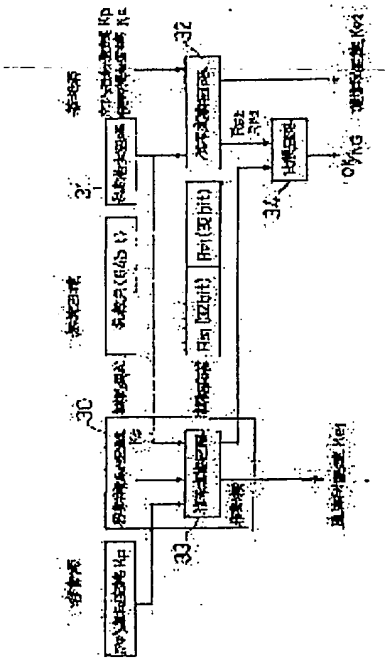
(51)Int.Cl. H04L 9/06
H04L 9/14
H04B 7/26

(21)Application number : 02-402926
(22)Date of filing : 17.12.1990

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
N T T IDOU TSUUSHINMOU KK
(72)Inventor : KAMIBAYASHI SHINJI
KOBAYASHI KATSUMI
ONOE SEIZO
HANAOKA MITSUAKI
NAKAMURA HIROSHI

(54) AUTHENTICATION METHOD IN DIGITAL MOBILE COMMUNICATION

(57)Abstract:
PURPOSE: To enable a mobile station to be shared and to prevent illegal use by specifying a authentication confirmation signal and a authentication reply signal of a mobile set and a subscriber with a random number and a secret key and starting the operation when both the signals are coincident.
CONSTITUTION: A random number generating circuit 31 generates at first a random number R for an authentication request in a base station and transmits the number to a mobile station. A mobile set 30 enters the random number R and secret keys Ks, Kp of the mobile set and subscriber to a signal conversion circuit 33 to obtain an authentication reply and a communication ciphering key Ke1 and transmits the authentication reply to the base station. The base station inputs the random number R and secret keys Ks, Kp to a signal conversion circuit 32 to obtain an authentication reply and a communication ciphering key Ke2. A comparator circuit 34 compares a bit pattern of the authentication reply received from the mobile station with a bit pattern of the authentication reply generated in the base station, and enables the authentication of the mobile set when they are coincident and disables the recognition in other cases. That is, then the authentication of the mobile set and the subscriber authentication are implemented simultaneously by one authentication procedure to share the mobile station by plural subscribers without degradation in the throughput.



LEGAL STATUS
[Date of request for examination] 29.11.1993
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number] 2555220
[Date of registration] 22.08.1996
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

CLAIMS

[Claim(s)]
[Claim 1] In the authentication approach in the digital mobile communication for judging whether in performing mobile communication between the migration machine by the side of a mobile station, and a base station, a communications partner is attested and a communication link is started Said mobile station creates a migration machine authentication reply signal according to the 1st specific principle with the predetermined random number sent from said base station, and the 1st private key of the migration machine proper currently held beforehand, and transmits it to this base station. According to the 2nd specific principle, create a subscriber authentication reply signal with this random number and the 2nd private key of the subscriber proper from a subscriber, and it transmits to this base station. The communication link secrecy key which keeps a communication link secret according to the 3rd specific principle with this random number and these 1st and 2nd private keys is created. Said base station With this predetermined random number generated in this base station, and said 1st and 2nd private keys currently held beforehand According to the said 1st, 2nd, and 3rd specific principles, a migration machine authentication acknowledge signal, a subscriber authentication acknowledge signal, and a communication link secrecy key are created. The authentication approach in the digital mobile communication characterized by performing delivery by said random number of this communication link secrecy key while comparing whether said migration machine authentication reply signal, this migration machine authentication acknowledge signal, and said subscriber authentication reply signal and this subscriber authentication acknowledge signal are in agreement and attesting said communications partner.
[Claim 2] The authentication approach in the digital mobile communication according to claim 1 characterized by replacing said a part of 2nd private key in said mobile station by said subscriber's recitation number.

[Translation done.]

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Industrial Application] This invention relates to the authentication approach in the digital mobile communication with which the base station in digital mobile communication attests that it is a mobile station with a communicative partner's just mobile station.
[0002]
[Description of the Prior Art] Protection of the security in the wireless section is strongly desired as the increment in mobile communication need and a demand of diversification of service increase in recent years. Generally, by mobile communication, a mobile station and a base station cannot judge the justification of the mobile station which communicates in a subscriber's accomodated location, in order that connection may change for every communication link. Therefore, while the authentication function for checking the justification of a mobile station is required, the authentication function of the subscriber who communicates is required of personal-communications number (PTN) service. Moreover, since a communication link is used for a wireless circuit, the secrecy function which the content of a communication link may be monitored and enciphers the content of a communication link for the security protection of the content of a communication link is required.
[0003] Here, drawing for explaining the conventional authentication approach to drawing 4 (A) and (B) is shown. Drawing 4 (A) and (B) show the delivery approach of the authentication in a ** yaw ROPPA automobile telephone system, and a communication link secrecy key. In drawing 4 (A), a fixed network side transmits a random number RAND (authentication demand signal) to a mobile station first. A mobile station is the key Ks of the authentication currently beforehand held in the mobile station in encryption circuit 51a according to algorithm A3, such as DES (Data Encryption Standard). SRES (authentication reply signal) is computed from a random number RAND, and it transmits to a fixed network side.
[0004] Key Ks of the authentication currently beforehand held by the fixed network side on the other hand at the random-number RAND and fixed network side In encryption circuit 51b (it is the same as encryption circuit 51a), SRES is computed according to algorithm A3. And in a comparison circuit 52, SRES computed by the fixed network side is compared with SRES transmitted from the mobile station, if it is coincidence (yes), a communication link will be started, and if it is an inequality (no), communicating will become impossible. That is, the justification of SRES which received by the fixed network side is checked, and a mobile station is attested.
[0005] Moreover, drawing 4 (B) shows the delivery approach of a communication link secrecy key, and delivery of a communication link secrecy key is performed to authentication and coincidence of drawing 4 (A). Setting to drawing 4 (B), a fixed network side is a random number RAND and the key Ks of authentication. The communication link secrecy key Ke is computed according to the algorithm A8 of encryption circuit 55b, and it stores in the storage section 56. On the other hand, it is the communication link secrecy key Ke by the side of a fixed network. It does not carry out transmitting to a mobile station as it is, but it transmits indirectly using a random-number RAND signal. Key Ks of a random number RAND and authentication in ******** and a mobile station The algorithm A8 of encryption circuit 55a is followed, and it is the communication link secrecy key Ke. It computes and stores in the storage section 57.
[0006] Thus, the encryption circuits 51a and 51b, algorithm A3 of 55a and 55b, and A8 By making it encryption algorithm, it is possible to prevent a third party's tapping and the activity of an unjust mobile station, and it can realize enciphering and delivering the secrecy key for keeping the communication link after authentication secret to authentication and coincidence.
[0007]
[Problem(s) to be Solved by the Invention] However, key Ks of authentication by the above-mentioned approach Since only one kind of authentication to depend is performed, the migration machine and subscriber by the side of a mobile station cannot be distinguished, for example, one set of a migration machine cannot be shared by two or more subscribers. However, although it was possible to have performed subscriber authentication and migration machine authentication independently by repeating the same procedure twice, since the amount of signals which carries out a radio transmission doubled and a throughput fell, there was a problem that the number of subscribers which can be held will become fewer. Moreover, key Ks of authentication Since it was held at the migration inside of a plane, when the body of a migration machine was stolen, there was a problem that an unjust activity was attained.
[0008] Then, while this invention was made in view of the above-mentioned technical problem, can prevent lowering of the throughput of wireless and can share one set of a mobile station by two or more subscribers, it aims at

offering the authentication approach in the digital mobile communication which prevents the unjust activity by the theft.

[0009]

[Means for Solving the Problem] In the authentication approach in the digital mobile communication for judging whether in performing mobile communication between the migration machine by the side of a mobile station, and a base station, the above-mentioned technical problem attests a communications partner, and starts a communication link Said mobile station creates a migration machine authentication reply signal according to the 1st specific principle with the predetermined random number sent from said base station, and the 1st private key of the migration machine proper currently held beforehand, and transmits it to this base station. According to the 2nd specific principle, create a subscriber authentication reply signal with this random number and the 2nd private key of the subscriber proper from a subscriber, and it transmits to this base station. The communication link secrecy key which keeps a communication link secret according to the 3rd specific principle with this random number and these 1st and 2nd private keys is created. Said base station With this predetermined random number generated in this base station, and said 1st and 2nd private keys currently held beforehand According to the said 1st, 2nd, and 3rd specific principles, a migration machine authentication acknowledge signal, a subscriber authentication acknowledge signal, and a communication link secrecy key are created. While comparing whether said migration machine authentication reply signal, this migration machine authentication acknowledge signal, and said subscriber authentication reply signal and this subscriber authentication acknowledge signal are in agreement and attesting said communications partner It is solved performing delivery by said random number of this communication link secrecy key, or by replacing said a part of 2nd private key in said mobile station by said subscriber's recitation number.

[0010]

[Function] As mentioned above, a migration machine authentication reply signal and a subscriber authentication reply signal are created for a predetermined random number from a base station with these random number and 1st and 2nd private keys with delivery and a mobile station to a mobile station. On the other hand, in a base station, a migration machine authentication acknowledge signal and a subscriber authentication acknowledge signal are created with this random number and the 1st and 2nd private keys currently held beforehand. And a communication link is started, when a reply signal and an acknowledge signal concerned are compared and it is in agreement in a base station.

[0011] That is, it becomes possible by performing migration machine authentication and subscriber authentication simultaneously in an authentication procedure once to share one set of a migration machine by two or more subscribers, without reducing the throughput of wireless. Moreover, by transposing a part of 2nd private key to a subscriber's recitation number, when the body of a migration machine is stolen, it becomes possible to prevent an unjust activity.

[0012] Moreover, a mobile station and a base station create a communication link secrecy key with a random number and the 1st and 2nd private keys. That is, when an above-mentioned reply signal and an above-mentioned acknowledge signal are in agreement, it means that the communication link secrecy key in both a mobile station and a base station was shared correctly. Therefore, it becomes possible to perform simultaneously migration machine authentication, subscriber authentication, and delivery of a communication link secrecy key.

[0013]

[Example] The block diagram of one example of this invention is shown in drawing 1 . Among drawing 1 , in a migration machine [in / in 30 / a mobile station], and 31, the signal transformation circuit of a base station and 33 carry out the signal transformation circuit of a mobile station, and, as for 34, the random-number-generation circuit of a base station and 32 are carrying out the table of the comparison circuit of a base station, respectively. The signal transformation circuits 32 and 33 are the same functional secrecy and Key Kp. It shares. A subscriber's private key Kp For example, it being recorded on an IC card etc. and inserting in the migration machine 30 at the time of an activity etc. is the gestalt which the migration machine 30 and the subscriber separated.

[0014] A base station is the random-number-generation circuit 31 first, generates the random number R for an authentication demand, and transmits it to a mobile station. The bit length of the viewpoint of code reinforcement to the random number R has desirable about 64 bits or more.

[0015] The migration machine 30 is the received private key Ks of a random number R and a migration machine. A subscriber's private key Kp read from the subscriber card It inputs into the signal transformation circuit 33, and the authentication responses Rs1 and Rp1 and the communication link secrecy key Ke1 are obtained. This communication link secrecy key Ke2 is used as a communication link secrecy key for keeping future communication links secret. And the authentication responses Rs1 and Rp1 are transmitted to a base station.

[0016] A base station is the random number R and private key Ks which were generated in the random-number-generation circuit 31. And Kp It inputs into the signal transformation circuit 32, and the authentication response Rs2, Rp2, and the communication link secrecy key Ke2 are obtained. The communication link secrecy key Ke2 is used as a communication link secrecy key for keeping future communication links secret. A comparison circuit 34 inputs the authentication responses Rs1 and Rp1 received from the mobile station, and the signals Rs2 and Rp2 generated in the base station, and compares each bit pattern (array of a bit string). When Rs1 and Rs2 are equal, it considers as the migration machine authentication O.K., and when other, it considers as the migration machine authentication NG. Moreover, when Rp1 and Rp2 are equal, it considers as the subscriber authentication O.K., and when other, it considers as the subscriber authentication NG. It is the private key Ks of a mobile station and a base station that each bit pattern is in agreement. And Kp The same thing (therefore, a communicative partner's mobile station is a

just mobile station) is meant, and what (therefore, the communication link secrecy key was shared correctly) the authentication demand and the authentication response were mistaken and was transmitted that there is nothing is guaranteed by the high probability (reliability becomes so high that R and the number of bits of Rs1 and Rp1 are... made [many]).

[0017] In addition, private key Kp of the subscriber of a mobile station A part is recorded on the nonvolatile memory in the migration machine 30, and a subscriber memorizes the remainder as a personal identification number, and when starting a communication link, it may be inputted into the migration machine 30 with a ten key etc. Moreover, you may be the case where the result obtained by a certain specific operation of a personal identification number and the number on memory is used as a private key. An unjust activity becomes impossible, if according to this a personal identification number is not known even if the migration machine 30 is stolen.

[0018] Next, the block diagram of one example of the signal transformation circuit in the migration machine of drawing 1 is shown in drawing 2 . Among the signal transformation circuit 33 of drawing 2 , in the 1st encryption circuit and 42, the 2nd encryption circuit and 43 express the 3rd code circuit, and 44 expresses [41] the multiplexing circuit, respectively. In addition, also in the signal transformation circuit 33 of a base station, it is the same configuration except for the multiplexing circuit 44. moreover, the 1- the same circuitry is sufficient as the 3rd encryption circuit.

[0019] The 1st encryption circuit 41 is a subscriber's private key Kp. It uses, the random number R for an authentication demand received from the base station is enciphered by 32 bits according to the 2nd specific principle, and the authentication response Rp1 is outputted. The 2nd code circuit 42 is the private key Ks of the migration machine 30. It uses, a random number R is enciphered by 32 bits according to the 1st specific principle, and the authentication response Rs1 is outputted. The 3rd encryption circuit 43 is the private key Ks of the migration machine 30. It uses, the authentication response Rs1 is enciphered according to the 3rd specific principle, and the communication link secrecy key Ke1 is outputted. Moreover, the multiplexing circuit 44 multiplexes Rs1 and Rp1, and outputs them to a base station as one signal. In addition, the multiplexing circuit 44 may be removed and Rs1 and Rp1 may be transmitted as another signal.

[0020] the 1- the code realized in the 3rd encryption circuit 41, 42, and 43 requires that circuit magnitude should be small and there should be few throughputs, in order to realize in the migration machine 30. such the 1- as a cipher system by the 3rd specific principle, private key cryptosystems, such as FEAL (Fast data Encipherment Algorithm) and DES, are effective. Therefore, it is actually impossible that deriving the above-mentioned code secrecy key Ke1 intercepts the communication link after authentication since it is actual very difficult, and to create and use an unjust mobile station. In addition, although the point of reliability is sufficient as making it the same as an input signal R, as long as the number of bits of output signals Rs1 and Rp1 has enough the large number of bits of an input signal R, it may make the number of bits of output signals Rs1 and Rp1 fewer than an input signal, and may raise the throughput of wireless. For example, although both the output signals Rs1 and Rp1 will become 64 bits like drawing 1 if an input signal R is made into 64 bits when adopting FEAL as a cipher system, only 32 bits of each low order are extracted and multiplexed, and a 64-bit authentication response is constituted and it transmits. According to this, it becomes much more difficult to compute a private key by intercepting. In addition, although the above-mentioned example was only expressed as the base station, it contains the control station of the high order of a base station, the exchange, a home memory station, etc.

[0021] Next, the block diagram of other examples of this invention is shown in drawing 3 . Drawing 3 (A) is what showed the outline in the case of attesting among users, and drawing 3 (B) is a block diagram for making drawing 3 (A) correspond to drawing 1 R> 1, and explaining it. In drawing 3 (A), it attests between an authentication invoking user (equivalent to the base station in drawing 1), and an attested side user (equivalent to the mobile station in drawing 1), and the cryptographic key Ki (equivalent to Kp [in drawing 1] and Ks) of secrecy is shared.

[0022] A now and authentication initiator user is Plaintext P and a cryptographic key Ki while transmitting the suitable plaintext P (equivalent to the random number R in drawing 1) to an attested side user. It uses and Code C (equivalent to Rs2 and Rp2 in drawing 1) is generated. The plaintext P which received by the attested side user on the other hand to cryptographic key Ki It uses, cipher C' (equivalent to Rs1 and Rp1 in drawing 1) is generated, and an authentication initiator user is returned. It is Authentication O.K. if Cipher C and C' are equal.

[0023] Thus, by making Plaintext P into a different sentence (random number) for every authentication, the content of the authentication procedure can be changed for every call, and secrecy nature can realize the high authentication approach.

[0024] Moreover, in drawing 3 (B), by the encryption machine F of encryption machine F' (equivalent to the signal transformation circuit 32 in drawing 1) of the migration exchange (authentication invoking user), and a migration machine (attested user), and F" (equivalent to the signal transformation circuit 33 in drawing 1), in order to make an encryption rate quick and to make small the burden to CPU (central processing unit) of a migration machine, secret key cryptosystems, such as the above-mentioned FEAL and DES, are used. in addition, authentication key Ki it is — authentication key Kp for subscribers And authentication key Ks for migration machines It stores in a home memory station as some subscriber datas.

[0025] First, the migration exchange transmits random-number R (P) generated within the migration exchange to a migration machine, and performs an authentication demand. So, in a migration machine, the encryption result Rp and Rs (C' in drawing 3 (A), and Rp1 and Rs12 in drawing 1 considerable) are obtained by the encryption machine F and F" using Kp which is an authentication key the object for subscribers, and for migration machines about R (P) which received, and Ks (Ki). It processes by taking out the authentication key Kp and Ks (Ki) from a home memory similarly

in the migration exchange.
[0026] And a migration machine is this encryption result Pp and Rs to the migration exchange. It transmits as an authentication response. By the migration exchange, comparison collating of both encryption result is carried out, when a result is in agreement, it is regarded as authentication normal, and a communication link is started. In addition, in drawing 2 , the secrecy key Ke1 is generated from the migration private key Ks, and it is the authentication key Kp for subscribers at drawing 3 (B). Although the secrecy key Ke1 is generated, both may not necessarily be another, and whichever is satisfactory for them as long as they are unified the migration exchange side.
[0027] Here, if the encryption result generated during an authentication procedure is used for a secrecy key (the secrecy key Ke1 of a migration machine, and secrecy key Ke2 of the migration exchange), since insurance and a secrecy key which could be realized efficiently and is different for every call are [delivery of the secrecy key in a wireless circuit] generable, a secrecy pattern can be changed for every call, and high secrecy of safety can do.
[0028]
[Effect of the Invention] As mentioned above, according to this invention, by being able to share one set of a migration machine by two or more subscribers, and making some private keys into a personal identification number in one authentication procedure, without lowering the throughput of wireless by realizing migration machine authentication and subscriber authentication simultaneously, even if a migration body is stolen, an unjust activity can be prevented by the personal identification number.

[Translation done.]

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] It is the block diagram of one example of this invention.
[Drawing 2] It is the block diagram of one example of signal exchange ****** in the migration machine of drawing 1 .

[Drawing 3] It is the block diagram of other examples of this invention.
[Drawing 4] It is drawing for explaining the conventional authentication approach.
[Description of Notations]
30 Migration Machine
31 Random-Number-Generation Circuit
32 33 Signal transformation circuit
34 Comparison Circuit
41 1st Encryption Circuit
42 2nd Encryption Circuit
43 3rd Encryption Circuit
44 Multiplexing Circuit

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平5－327693

(43)公開日　平成5年(1993)12月10日

(51)Int.Cl.[5]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ	9/06					
	9/14					
Ｈ０４Ｂ	7/26	１０９	Ｓ 7304－5Ｋ			
			7117－5Ｋ	Ｈ０４Ｌ	9／02	Ｚ

審査請求　未請求　請求項の数２(全 8 頁)

(21)出願番号　特願平2－402926

(22)出願日　平成２年(1990)12月17日

特許法第30条第１項適用申請有り　1990年９月15日　社団法人電子情報通信学会発行の「1990年電子情報通信学会秋季全国大会講演論文集」に発表

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区内幸町一丁目１番６号
(74)上記１名の代理人　弁理士　伊東　忠彦
(71)出願人　392026693
エヌ・ティ・ティ移動通信網株式会社
東京都港区虎ノ門二丁目10番１号
(72)発明者　上林　真司
東京都千代田区内幸町一丁目１番６号　日本電信電話株式会社内
(72)発明者　小林　勝美
東京都千代田区内幸町一丁目１番６号　日本電信電話株式会社内

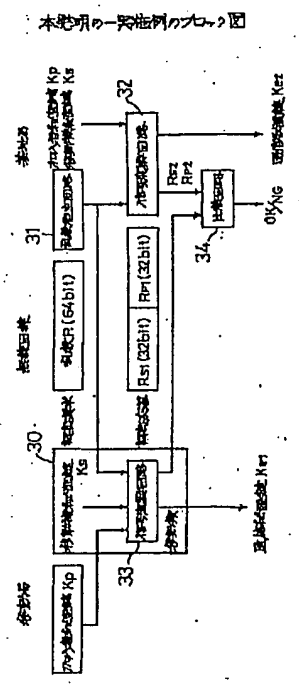
最終頁に続く

(54)【発明の名称】　ディジタル移動通信における認証方法

(57)【要約】

【目的】　本発明はディジタル移動通信における基地局が、通信の相手の移動局が正当な移動局であることを認証するディジタル移動通信における認証方法に関し、無線のスループットの低下を防止して１台の移動機を複数の加入者で共用することができると共に、盗難による不当な使用を防止することを目的とする。

【構成】　移動局において、基地局から送られた乱数Ｒと移動機秘密鍵Ｋs 及び加入者秘密鍵Ｋp より認証応答信号Ｒs1，Ｒp1を生成して基地局に送ると共に秘匿鍵ｋe1を生成する。一方、基地局においても同様にして認証確認信号Ｒs2，Ｒp2を生成して、認証応答信号Ｒs1，Ｒp1と比較し、一致すれば通信を開始するように構成する。また、基地局においても同様にして秘匿鍵Ｋe2を生成する。さらに、秘匿鍵の一部を暗証番号と置換える。



1

【特許請求の範囲】

【請求項1】　移動局側の移動機と基地局との間で移動通信を行うにあたり、通信相手の認証を行い、通信を開始するか否かの判断を行うためのディジタル移動通信における認証方法において、

前記移動局は、

前記基地局より送られた所定の乱数と、予め保持されている移動機固有の第1の秘密鍵とにより第1の特定法則に従って移動機認証応答信号を作成して該基地局に送信し、

該乱数と加入者からの加入者固有の第2の秘密鍵とにより第2の特定法則に従って加入者認証応答信号を作成して該基地局に送信し、

該乱数と該第1及び第2の秘密鍵とにより第3の特定法則に従って通信を秘匿する通信秘匿鍵を作成し、

前記基地局は、

該基地局で発生させた該所定の乱数と、予め保持されている前記第1及び第2の秘密鍵とにより、前記第1，第2及び第3の特定法則に従って移動機認証確認信号、加入者認証確認信号及び通信秘匿鍵を作成し、

前記移動機認証応答信号と該移動機認証確認信号、及び前記加入者認証応答信号と該加入者認証確認信号が一致するか否かを比較して前記通信相手を認証すると共に、該通信秘匿鍵の前記乱数による配送を行うことを特徴とするディジタル移動通信における認証方法。

【請求項2】　前記移動局における前記第2の秘密鍵の一部を、前記加入者の暗唱番号で置換えることを特徴とする請求項1記載のディジタル移動通信における認証方法。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、ディジタル移動通信における基地局が、通信の相手の移動局が正当な移動局であることを認証するディジタル移動通信における認証方法に関する。

【0002】

【従来の技術】近年、移動通信需要の増加、サービスの多様化の要求が高まるにつれて無線区間におけるセキュリティの保護が強く望まれている。一般に移動通信では、移動局と基地局とが通信毎に接続が変化するために、通信する移動局の正当性を加入者の収容位置で判定することができない。そのため、移動局の正当性をチェックするための認証機能が必要であると共に、パーソナル通信番号（ＰＴＮ）サービスでは通信を行う加入者の認証機能が必要である。また、無線回線を通信を用いることから通信内容を傍受される可能性があり、通信内容の機密保持のために通信内容を暗号化する秘匿機能が必要である。

【0003】ここで、図4（A），（B）に、従来の認証方法を説明するための図を示す。図4（A），（B）

2

は、汎ヨーロッパ自動車電話方式における認証及び通信秘匿鍵の配送方法を示したものである。図4（A）において、まず、固定網側は、乱数ＲＡＮＤ（認証要求信号）を移動局へ送信する。移動局は暗号化回路51aにおいて、ＤＥＳ（Data Encryption Standard）等のアルゴリズムA3に従い、予め移動局内に保持されている認証の鍵Ks と乱数ＲＡＮＤとからＳＲＥＳ（認証応答信号）を算出し、固定網側へ送信する。

【0004】一方、固定網側では乱数ＲＡＮＤと、固定網側に予め保持されている認証の鍵Ki とを暗号化回路51b（暗号化回路51aと同じ）においてアルゴリズムA3に従いＳＲＥＳを算出する。そして、比較回路52において、固定網側で算出したＳＲＥＳと移動局から送信されたＳＲＥＳとを比較し、一致（ｙｅｓ）であれば通信が開始され、不一致（ｎｏ）であれば通信不能となる。すなわち、固定網側で受信したＳＲＥＳの正当性を確認して、移動局の認証を行うものである。

【0005】また、図4（B）は通信秘匿鍵の配送方法を示すもので、通信秘匿鍵の配送は、図4（A）の認証と同時に行われる。図4（B）において、固定網側は乱数ＲＡＮＤと認証の鍵Ki とにより暗号化回路55bのアルゴリズムA8に従って通信秘匿鍵Ｋｅを算出して記憶部56にストアする。一方、固定網側の通信秘匿鍵Ｋｅをそのまま移動局へ送信することはせず、乱数ＲＡＮＤ信号を用いて間接的に送信する。すわなち、移動局では乱数ＲＡＮＤと認証の鍵Ks とを暗号化回路55aのアルゴリズムA8に従って通信秘匿鍵Ke を算出し、記憶部57にストアするものである。

【0006】このように、暗号化回路51a，51b及び55a，55bのアルゴリズムA3及びA8 を暗号化アルゴリズムにすることにより、第三者の盗聴及び不当な移動局の使用を防ぐことが可能であり、かつ、認証以後の通信を秘匿するための秘匿鍵を暗号化して配送することを認証と同時に実現できる。

【0007】

【発明が解決しようとする課題】しかし、上述の方法では認証の鍵Ks による1種類の認証しか行わないため、移動局側の移動機と加入者を区別できず、例えば1台の移動機を複数の加入者で共用することができない。ただ、同じ手順を2回繰り返すことにより、加入者認証と移動機認証を別々に行うことは可能であるが、無線伝送する信号量が2倍になり、スループットが低下するため、収容できる加入者数が減ってしまうという問題があった。また、認証の鍵Ki は、移動機内に保持されているため、移動機本体が盗まれた場合、不当な使用が可能になるという問題があった。

【0008】そこで、本発明は上記課題に鑑みなされたもので、無線のスループットの低下を防止して1台の移動局を複数の加入者で共用することができると共に、盗難による不当な使用を防止するディジタル移動通信にお

ける認証方法を提供することを目的とする。

【0009】

【課題を解決するための手段】上記課題は、移動局側の移動機と基地局との間で移動通信を行うにあたり、通信相手の認証を行い、通信を開始するか否かの判断を行うためのディジタル移動通信における認証方法において、前記移動局は、前記基地局より送られた所定の乱数と、予め保持されている移動機固有の第1の秘密鍵とにより第1の特定法則に従って移動機認証応答信号を作成して該基地局に送信し、該乱数と加入者からの加入者固有の第2の秘密鍵とにより第2の特定法則に従って加入者認証応答信号を作成して該基地局に送信し、該乱数と該第1及び第2の秘密鍵とにより第3の特定法則に従って通信を秘匿する通信秘匿鍵を作成し、前記基地局は、該基地局で発生させた該所定の乱数と、予め保持されている前記第1及び第2の秘密鍵とにより、前記第1，第2及び第3の特定法則に従って移動機認証確認信号、加入者認証確認信号及び通信秘匿鍵を作成し、前記移動機認証応答信号と該移動機認証確認信号、及び前記加入者認証応答信号と該加入者認証確認信号が一致するか否かを比較して前記通信相手を認証すると共に、該通信秘匿鍵の前記乱数による配送を行うことにより、または前記移動局における前記第2の秘密鍵の一部を、前記加入者の暗唱番号で置換えることにより解決される。

【0010】

【作用】上述のように、基地局より所定の乱数を移動局に送り、移動局でこの乱数と第1及び第2の秘密鍵とにより移動機認証応答信号及び加入者認証応答信号を作成する。一方、基地局では該乱数と予め保持されている第1及び第2の秘密鍵とにより移動機認証確認信号及び加入者認証確認信号を作成する。そして、基地局で当該応答信号と確認信号とを比較して、一致した場合に通信を開始するものである。

【0011】すなわち、一度の認証手順で移動機認証と加入者認証を同時に行うことにより、無線のスループットを低下させることなく1台の移動機を複数の加入者で共用することが可能となる。また、第2の秘密鍵の一部を加入者の暗唱番号に置換えることにより、移動機本体が盗まれた場合に不当な使用を防止することが可能となる。

【0012】また、移動局及び基地局は、乱数と第1及び第2の秘密鍵により通信秘匿鍵を作成する。すなわち、上述の応答信号及び確認信号が一致した場合には、移動局及び基地局両方における通信秘匿鍵が正しく共有されたこととなる。従って、移動機認証、加入者認証及び通信秘匿鍵の配送を同時に行うことが可能となる。

【0013】

【実施例】図1に、本発明の一実施例のブロック図を示す。図1中、30は移動局における移動機、31は基地局の乱数発生回路、32は基地局の信号変換回路、33は移動局の信号変換回路、34は基地局の比較回路をそれぞれ表している。信号変換回路32と33は同じ機能秘密，鍵Kp を共有する。加入者の秘密鍵Kp，は、例えば、ICカード等に記録され，使用時に移動機30に挿入する等，移動機30と加入者が分離した形態である。

【0014】基地局は、まず乱数発生回路31で、認証要求用の乱数Rを発生し、移動局へ送信する。暗号強度の観点から、乱数Rのビット長は64ビット程度以上が望ましい。

【0015】移動機30は、受信した乱数Rと、移動機の秘密鍵Ks と、加入者カードから読み出した加入者の秘密鍵Kp を信号変換回路33に入力し、認証応答Rs1，Rp1及び通信秘匿鍵Ke1を得る。この通信秘匿鍵Ke2は以後の通信を秘匿するための通信秘匿鍵として用いる。そして、認証応答Rs1，Rp1は基地局へ送信される。

【0016】基地局は、乱数発生回路31で発生した乱数Rと秘密鍵Ks 及びKp を信号変換回路32に入力し、認証応答Rs2，Rp2及び通信秘匿鍵Ke2を得る。通信秘匿鍵Ke2は以後の通信を秘匿するための通信秘匿鍵として用いる。比較回路34は、移動局から受信した認証応答Rs1，Rp1、及び基地局内で発生した信号Rs2，Rp2を入力し、それぞれのビットパターン（ビット列の配列）を比較する。Rs1とRs2が等しいとき移動機認証OKとし、それ以外のとき移動機認証NGとする。又Rp1とRp2が等しいとき加入者認証OKとし、それ以外のとき加入者認証NGとする。それぞれのビットパターンが一致するということは、移動局と基地局の秘密鍵Ks 及びKp が同じである（従って通信の相手の移動局が正当な移動局である）ことを意味し、認証要求と認証応答が誤り無く伝送された（従って通信秘匿鍵が正しく共有された）ことを高い確率で保証する（信頼度はRとRs1及びRp1のビット数を多くする程高くなる）。

【0017】なお、移動局の加入者の秘密鍵Kp は，一部を移動機30内の不揮発性メモリに記録し、残りは加入者が暗証番号として記憶し、通信を開始するとき等にテンキー等により移動機30に入力してもよい。また、暗証番号とメモリ上の番号との、ある特定の演算で得られる結果を秘密鍵とする場合であってもよい。これによれば、移動機30が盗まれても暗証番号がわからなければ、不当な使用が不可能になる。

【0018】次に、図2に、図1の移動機における信号変換回路の一具体例のブロック図を示す。図2の信号変換回路33中、41は第1の暗号化回路、42は第2の暗号化回路，43は第3の暗号回路，44は多重化回路をそれぞれ表わしている。なお、基地局の信号変換回路33においても多重化回路44を除き同じ構成である。また、第1～第3の暗号化回路は同一の回路構成でもよい。

【0019】第1の暗号化回路41は、加入者の秘密鍵

Kp を用いて、基地局から受信した認証要求用の乱数Rを第2の特定法則に従い32ビットで暗号化し、認証応答Rp1を出力する。第2の暗号回路42は、移動機30の秘密鍵Ks を用いて乱数Rを第1の特定法則に従い、32ビットで暗号化し、認証応答Rs1を出力する。第3の暗号化回路43は、移動機30の秘密鍵Ks を用いて、認証応答Rs1を第3の特定法則に従い、暗号化し、通信秘匿鍵Ke1を出力する。また、多重化回路44は、Rs1とRp1を多重化し、一信号として基地局に出力する。なお、多重化回路44を外し、Rs1とRp1を別信号として送信してもよい。

【0020】第1～第3の暗号化回路41，42及び43で実現する暗号は、移動機30内実現するため、回路規模が小さく処理量が少ないことが必要である。このような第1～第3の特定法則による暗号化方式としては例えばFEAL (Fast data Encipherment Algorithm)，DES等の秘密鍵暗号方式が有効である。従って、上記の暗号秘匿鍵Ke1を導出することが現実に極めて困難なため、認証以降の通信を盗聴すること、及び不当な移動局を作成して使用することが、現実的には不可能である。なお、出力信号Rs1，Rp1のビット数は入力信号Rとは同じにするのが信頼度の点で良いが、入力信号Rのビット数が充分大きければ、出力信号Rs1，Rp1のビット数を入力信号より少なくし、無線のスループットを向上させてもよい。例えば、暗号方式としてFEALを採用する場合、図1のように、入力信号Rを64ビットとすると出力信号Rs1，Rp1は共に64ビットとなるが、それぞれの下位32ビットのみを抽出し、多重化して64ビットの認証応答を構成して送信する。これによれば、盗聴して秘密鍵を算出することが一層困難になる。なお、上記実施例は、単に基地局と表現したが、基地局の上位の制御局，交換局，ホームメモリ局等を含む。

【0021】次に、図3に、本発明の他の実施例のブロック図を示す。図3（A）はユーザ間で認証を行う場合の概要を示したもので、図3（B）は、図3（A）を図1に対応させて説明するためのブロック図である。図3（A）において、認証起動ユーザ（図1における基地局に相当）と被認証側ユーザ（図1における移動局に相当）間で認証を行うもので、秘密の暗号鍵Ki （図1におけるKp，Ks に相当）を共有する。

【0022】いま、認証起動側ユーザは適当な平文P（図1における乱数Rに相当）を被認証側ユーザに送信すると共に、平文Pと暗号鍵Ki を用いて暗号C（図1におけるRs2，Rp2に相当）を生成する。一方、被認証側ユーザでは、受信した平文Pから暗号鍵Ki を用いて暗号文C'（図1におけるRs1，Rp1に相当）を生成し、認証起動側ユーザに返送する。暗号文CとC'が等しければ認証OKである。

【0023】このように、平文Pを認証毎に異なった文（乱数）にすることにより、認証手順の内容を呼毎に変えることができ、秘匿性が高い認証方法を実現することができる。

【0024】また、図3（B）において、移動交換機（認証起動ユーザ）の暗号化器F'（図1における信号変換回路32に相当）及び移動機（被認証ユーザ）の暗号化器F，F"（図1における信号変換回路33に相当）では、暗号化速度を速くし、移動機のCPU（中央処理装置）に対する負担を小さくするために、前述のFEAL、DES等の秘密鍵暗号を用いる。なお、認証鍵Ki である加入者用認証鍵Kp 及び移動機用認証鍵Ksは加入者データの一部としてホームメモリ局に格納する。

【0025】まず、移動交換機は移動機に対して、移動交換機内で発生した乱数R（P）を送信して認証要求を行う。そこで、移動機では、受信したR（P）を加入者用と移動機用の認証鍵であるKp，Ks （Ki ）を用いて暗号化器F及びF"にて暗号化結果Rp，Rs （図3（A）におけるC'，図1におけるRp1，Rs12 相当）を得る。移動交換機においても同様にホームメモリより認証鍵Kp，Ks （Ki ）を取出して処理を行う。

【0026】そして、移動機は移動交換機に該暗号化結果Pp，Rs を認証応答として送信する。移動交換機では両者の暗号化結果を比較照合し、結果が一致した場合に認証正常とみなして、通信を開始するものである。なお、図2では移動秘密鍵Ksより秘匿鍵Ke1を生成しており、図3（B）では加入者用認証鍵Kp より秘匿鍵Ke1を生成しているが、両者は必ずしも別のものではなく、移動交換機側と統一されていればどちらでもよい。

【0027】ここで、認証手順中に生成される暗号化結果を秘匿鍵に利用すれば（移動機の秘匿鍵Ke1及び移動交換機の秘匿鍵Ke2）、無線回線における秘匿鍵の配送を安全かつ効率的に実現でき、また呼毎に異なった秘匿鍵を生成できることから秘匿パターンを呼毎に変えられ、安全性の高い秘匿ができる。

【0028】

【発明の効果】以上のように本発明によれば、1回の認証手順で、移動機認証と加入者認証を同時に実現することにより、無線のスループットを下げることなく、1台の移動機を複数の加入者で共用することができ、秘密鍵の一部を暗証番号とすることにより、移動本体が盗まれても暗証番号により不当な使用を防止することができる。

【図面の簡単な説明】

【図1】本発明の一実施例のブロック図である。

【図2】図1の移動機における信号交換換回路の一具体例のブロック図である。

【図3】本発明の他の実施例のブロック図である。

【図4】従来の認証方法を説明するための図である。

【符号の説明】

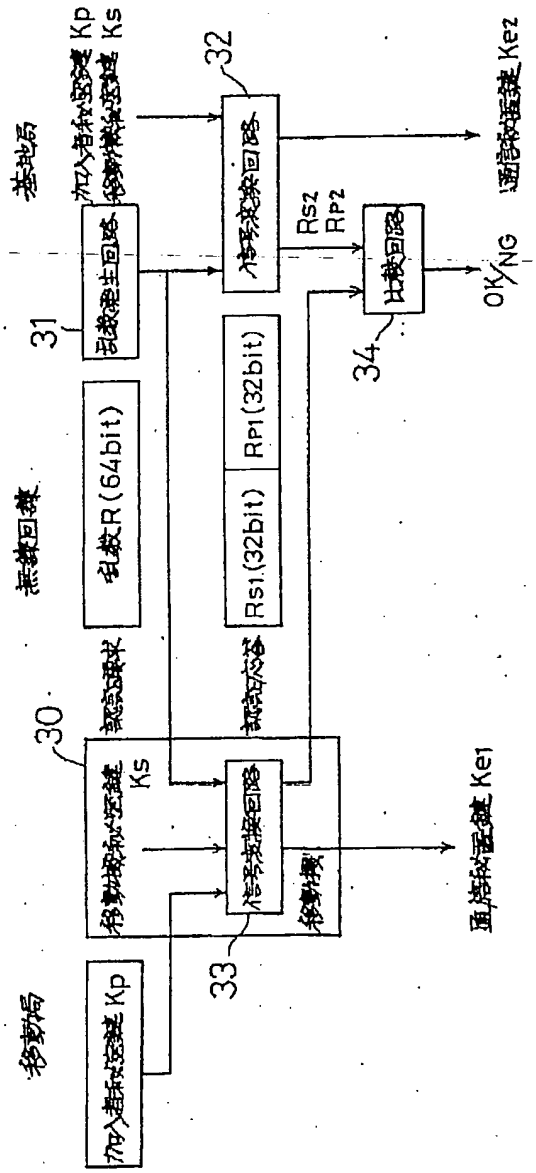
30　移動機

7　　8

31　乱数発生回路
32，33　信号変換回路
34　比較回路
41　第1の暗号化回路
42　第2の暗号化回路
43　第3の暗号化回路
44　多重化回路

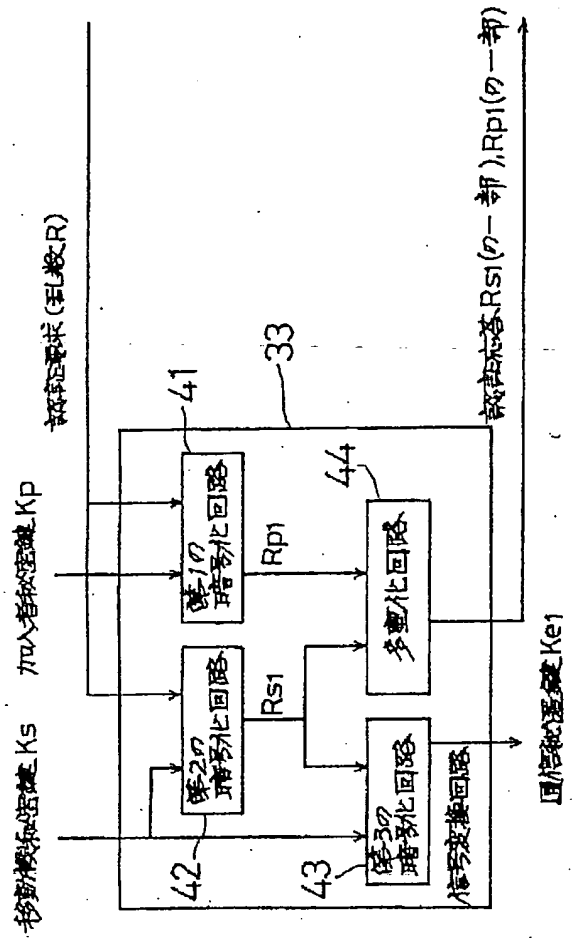
【図1】

本発明の一実施例のブロック図



【図2】

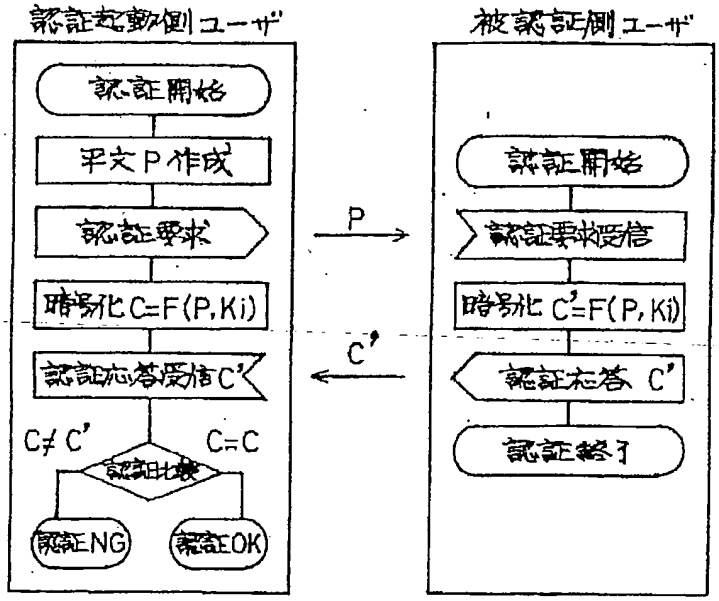
図1の移動機における信号変換回路の一具体例のブロック図



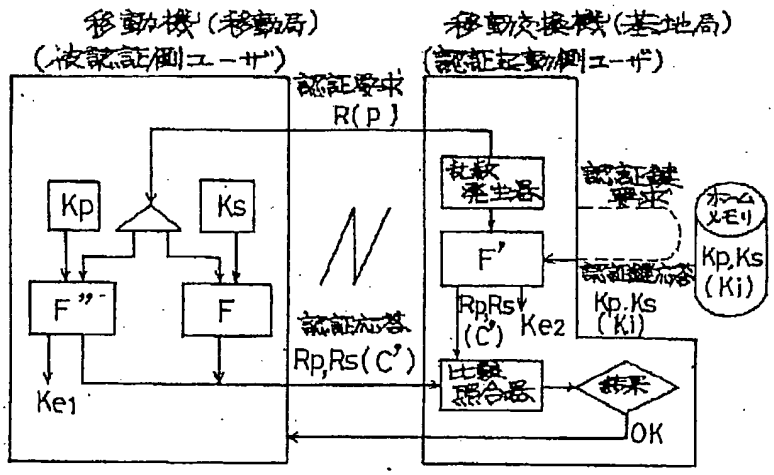
【図3】

本発明の他の実施例のブロック図

(A)

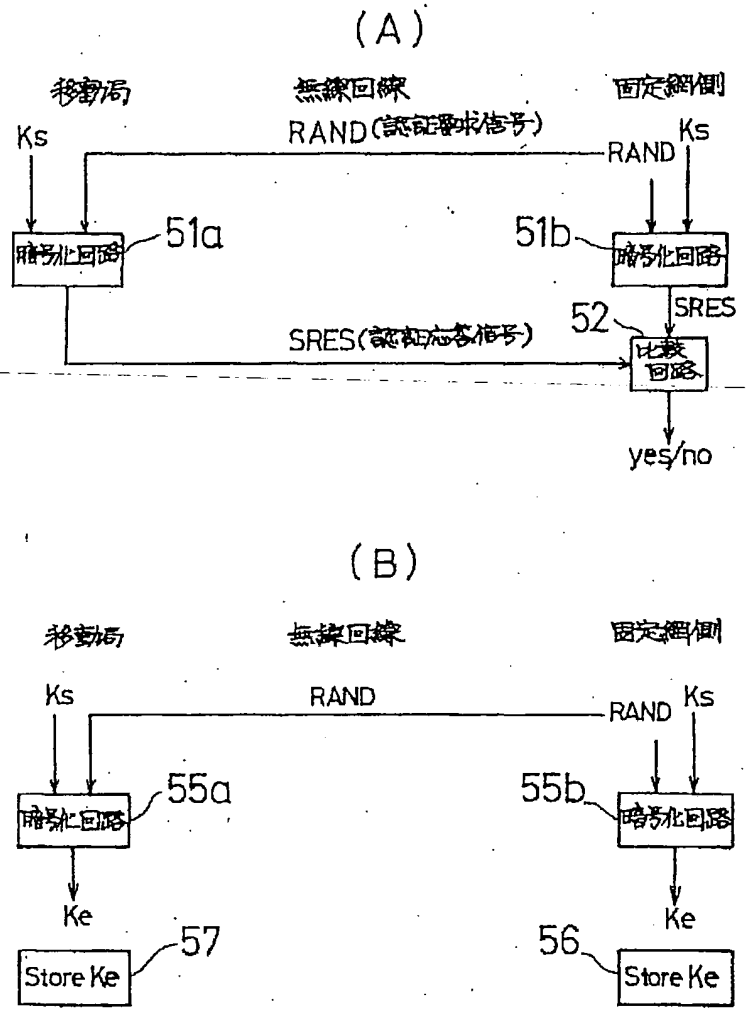


(B)



【図4】

従来の認証方法を説明するための図



フロントページの続き

(72)発明者　尾上　誠蔵
東京都千代田区内幸町一丁目1番6号　日本電信電話株式会社内

(72)発明者　花岡　光昭
東京都千代田区内幸町一丁目1番6号　日本電信電話株式会社内

(72)発明者　中村　寛
東京都千代田区内幸町一丁目1番6号　日本電信電話株式会社内